Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Service Rules for the 698-746, 747-762 and 777-792 MHz Bands	)	WT Docket No. 06-150
	)	
	)	
Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band	)	PS Docket No. 06-229
	)	
	)	
Amendment of Part 90 of the Commission's Rules	)	WP Docket No. 07-100
	)	

To: The Commission

COMMENTS OF SYNIVERSE TECHNOLOGIES

Syniverse Technologies ("Syniverse") commends the Commission for moving forward on the development of a framework for interoperable public safety broadband communications in the 700 MHz band. In particular, this *Notice* is an important step towards determining several key governance issues necessary to advance the deployment of an interoperable public safety broadband network.[1] To assist the Commission as it considers issues related to roaming and interconnection among public safety users and systems, Syniverse offers these comments based on over 20 years of experience in helping wireless operators roam and interconnect in the commercial marketplace. Syniverse supports adoption of a clearing house function to facilitate

[1] Service Rules for the 698-746, 747-762 and 777-792 MHz Bands; Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band; Amendment of Part 90 of the Commission's Rules, WT Docket no. 06-150, PS Docket No. 06-229, WP Docket No. 07-100, *Third Report and Order and Fourth Further Notice of Proposed Rulemaking*, 26 FCC Rcd 733 (2011) (the "*Notice*").

roaming and use of a third-party IP Packet Exchange ("IPX") solution to achieve interconnectivity.

I. INTRODUCTION

The Commission's actions this past January are significant milestones in the advancement of interoperable public safety broadband communications. By adopting Long Term Evolution ("LTE") as the communications technology platform for the 700 MHz public safety broadband spectrum, public safety will not only benefit from economies of scale – with access to commercial, off-the-shelf equipment – but also from innovation in the LTE space. The *Notice* sets the course for governance issues to make true interoperability a reality. Syniverse provides these comments in furtherance of this goal.

Syniverse makes wireless work through its messaging, roaming, and network and database solutions. Headquartered in Tampa, Florida with offices in major cities around the globe, Syniverse is the leading enabler of wireless voice and data services worldwide, connecting more than 900 communications providers and businesses in over 160 countries and reaching more than 1.7 billion mobile subscribers.

Syniverse plays a critical role connecting the world's growing number of roaming partners. The company processes vital and sensitive operator interactions, regardless of technology type, billing format or signaling standard. The solutions include roaming hub, data clearing, financial clearing and settlement, and fraud management services. Syniverse's suite of transaction-based services allows commercial wireless providers to deliver seamless voice, data and next generation services to wireless subscribers, including wireless voice and data roaming, Short Message Service ("SMS"), Multimedia Messaging Services ("MMS"), number portability and value-added roaming services. In addition, Syniverse facilitates full voice and data connectivity among mobile, fixed and broadband networks. By translating incompatible

communication standards and protocols, Syniverse makes it possible for different networks, disparate technologies, and multiple standards to interoperate.

II. A ROAMING CLEARING HOUSE WILL ENABLE EFFECTIVE AND EFFICIENT PUBLIC SAFETY ROAMING CAPABILITES.

Roaming has been an important and successful element of the commercial mobile service market for decades. Public safety can benefit from this experience and achieve significant efficiencies by modeling roaming solutions that are already available in the marketplace, including the use of a clearing house model, as the *Notice* envisions. Syniverse thus agrees with the Commission's tentative conclusion that a third party clearing house performing authentication and clearing functions is more efficient than having individual public safety operators performing these functions.[2]

There is no need to create an entirely new framework for public safety roaming. The commercial sector has already established and implemented procedures, guidelines, and clearing houses to enable this capability. Even with recently-deployed 4G LTE technology, the GSM Association ("GSMA") is involved with implementing a process for roaming among the LTE networks: starting first with network setup and negotiations over roaming agreements, operators can go through network and billing testing to make ready for the eventual launch of roaming services; the GSMA has also developed templates to guide roaming negotiations, has crafted technical guidelines so that LTE networks can interwork to provide end users with next generation capabilities when roaming, and continues to make progress on the various

[2] *Notice*, 26 FCC Rcd at 745 ¶ 37.

components of LTE roaming.[3] This body of work is easily transferable for use by regional and tribal public safety networks.

The clearing house model is a critical part of the roaming process in the commercial sector and is used extensively to centralize a full range of offerings that can handle virtually all tasks related to roaming data clearing. For example, Syniverse has developed a roaming hub services solution that enables operators to access a suite of comprehensive roaming services through a single entry point. Via the roaming hub, an operator need only establish a single agreement with Syniverse rather than multiple (hundreds) of bilateral agreements with other networks. On the technical side, an operator need only plan, design, establish and maintain the technical connectivity to Syniverse. The hub then provides operators with access to all Syniverse roaming services, including agreement management, data and financial clearing, and fraud prevention. The Syniverse solution is IPv4 – and IPv6 – compatible and can support home-routed and local breakout roaming.

With the ever-increasing volume of roaming data generated, and the importance of capturing all revenue accurately, operators increasingly rely on clearing houses to provide a secure, reliable and efficient way to clear and settle transferred account procedures ("TAP") records. By integrating authentication and clearing functions within a clearing house, significant efficiencies are created because operators do not individually need to integrate such functionality with each roaming party. The administrative, operational and developmental costs of enabling roaming and interoperability are therefore reduced. A clearing house also provides the additional benefit of giving operators a neutral entity for reporting and dispute resolution. The clearing

[3] *See* GSMA, *GSMA PRD IR.88 – "LTE Roaming Guidelines" 3.1* (Feb. 17, 2011), http://www.gsmworld.com/documents/IR8831.PDF; Reinhard Kreft, *LTE Roaming, A Solid Step Forward*, WIN-WIN, Aug. 2010, at 28, http://www.huawei.com/file/download.do?f=6824.

house model that is successfully used for the commercial wireless industry can work equally well to facilitate roaming among regional and tribal public safety networks.

In the *Notice*, the Commission asks whether there should be a single or multiple clearing houses.[4] The question of how simple or complex to make the design of interoperable public safety communications among disparate networks is within the Commission's discretion, and Syniverse does not comment on that issue here. It should be noted, however, that if the Commission decides to have multiple clearing houses, then there will need to be peering arrangements between the exchanges and additional testing to ensure the networks and billing capabilities are functioning properly before going "live." This inevitably increases the costs of operating an interoperable network.

III. PUBLIC SAFETY NETWORK OPERATORS CAN, AND SHOULD, USE A THIRD-PARTY IPX SOLUTION TO ACHIEVE INTERCONNECTIVITY WITH OTHER OPERATORS.

To achieve interconnectivity among public safety operators, the Commission asks whether a clearing house model, using the IPX protocol, can provide a secure and reliable solution that is cost effective.[5] On this issue, the answer is an emphatic yes.

The commercial marketplace has spurred the deployment of state-of-the-art private IP backbone capabilities that can be leveraged to provide regional and tribal public safety network operators with interconnectivity and much, much more. In 2006, the GSMA defined a standardized interconnection service specification, known as the IPX, to provide industry with a commercial and technical solution to manage IP traffic. Designed as the next evolution of the

[4] *Notice*, 26 FCC Rcd at 745 ¶ 37.

[5] *Id*. at 746 ¶ 41.

GSMA's GPRS Roaming Exchange ("GRX") service, the global IPX network went live in 2008, and Syniverse launched its IPX network transport solution in early 2009.[6]

The IPX network architecture consists of separate and competing network operators ("IPX providers"), like Syniverse, that connect with each other to exchange traffic through peering arrangements, forming a private IP backbone. The IPX providers, in turn, offer interconnect capability for IPX services to any service provider that agrees to adopt the necessary technical and commercial IPX principles. Participating providers can include GSM/CDMA/WiMax/LTE mobile network operators, fixed network operators, Internet service providers, and application service providers.

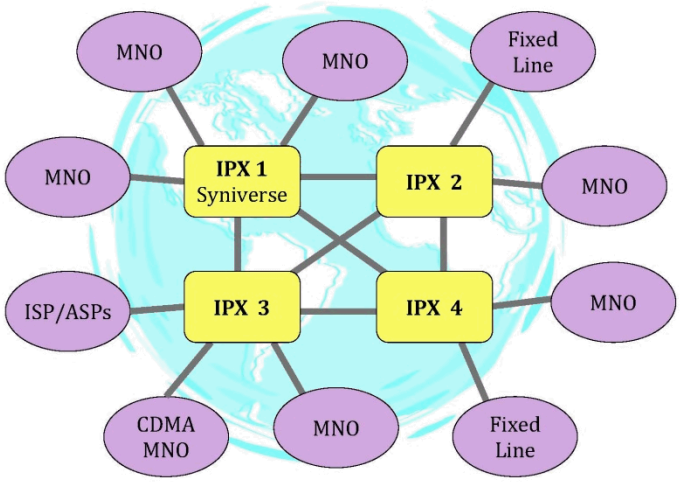

Figure 1. The IPX Network Architecture.

With a single connection to an IPX provider, a mobile network operator can either connect bilaterally with another operator or have a multilateral interconnection with hundreds of

[6] *See* News Release, GSMA, *High-Quality Global IP Network Prepares To Go Commercial* (Feb. 12, 2008), http://gsmworld.com/newsroom/press-releases/2008/859.htm; Press Release, Syniverse, Syniverse Launches Global IPX Network Transport Solution (Feb. 3, 2009), http://www.syniverse.com/press-releases/2009/global-IPX-network-transport-solution.

participating operators around the nation and the world.[7] The interconnection service available varies and can include: (1) transport – the transfer of IP data packets between two or multiple operators with an end-to-end quality of service ("QoS") guarantee; (2) service transit – both transport and service-aware cascaded billing capabilities, enabling all responsible participants in the transit chain to receive a commercial return for their participation; and (3) service hub – a multilateral connection with service-aware cascaded billing capabilities, enabling traffic exchange and service interworking between participating service providers. The different combinations give service providers flexible connectivity options.

The IPX network can deliver many different services and applications among operators, in addition to roaming. For example, Syniverse's IPX solution not only provides IPX transport services for signaling – CDMA/GPRS/LTE roaming, WLAN roaming, and message interworking (MMS, SMS) – but also provides IPX interworking services for IP voice telephony, video telephony, push-to-talk over cellular and advanced messaging and presence.

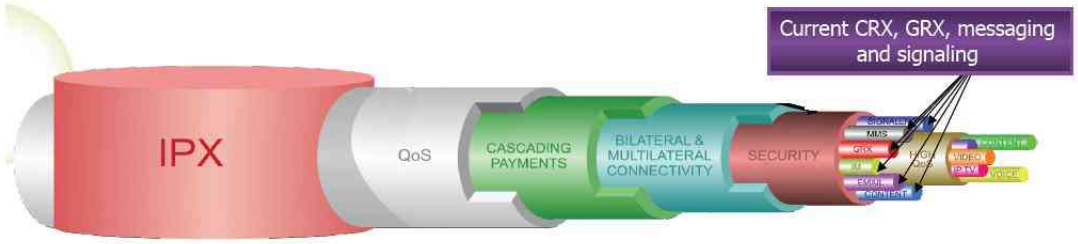

Figure 2. The IPX Network – Multiple Services over One Network.

[7] The GSMA provides a template agreement detailing the general terms and conditions in the provision of IPX services between IPX and service providers. *See* GSMA, *Agreement for IP Packet eXchange (IPX) Services 3.0*, July 2008, http://www.gsmworld.com/documents/aa80_3_0.pdf.

Critical to commercial and public safety operators alike, the IPX solution can provide future and backward compatibility. While all operators may start out using the same LTE technology, some systems will evolve faster than others. Like the private sector, public safety will need a solution that ensures interoperable communications between legacy and next generation systems.

Moreover, the IPX solution can provide the necessary financial clearing and settlement functions for public safety network operators. All sessions flowing across an IPX interconnect go through a proxy, like Diameter, producing Call Detail Records ("CDRs") to facilitate interconnect billing and cascade payments. The CDRs may contain information such as the duration of the session, type of media and codec, type of application, bandwidth and throughput consumed, etc. This provides a comprehensive view of resource utilization for billing purposes. The CDRs are turned into a TAP record, which is rated and placed in a TAP file and sent to a data clearing house for settlement purposes.

In the *Notice*, the Commission asks about the "performance, reliability, and security" of the private IPX network and whether it is cost effective.[8] The IPX is a premium quality all-in-one solution that is very reliable and secure. All connecting parties to the IPX network execute a commercial agreement providing for a security code of conduct and specified QoS levels. Each party in the transmission chain is thus responsible for the performance and service they provide. Because the private IPX backbone is separate and apart from the Internet, the network is protected from malicious attacks and spam – end user terminals are unable to probe the core networks involved in the management and delivery of the IP services. With individual operator traffic segregated, any security breaches are localized.

[8] *See Notice*, 26 FCC Rcd at 746 ¶ 41.

Use of an IPX provider will create significant efficiencies for public safety, reducing the cost of developing and operating the interoperable broadband network. For example, by consolidating the network intelligence needed for roaming and interoperable communications in an IPX provider's central hub, public safety can forgo the cost of deploying such capabilities in their individual core networks. In addition, use of an IPX provider simplifies the network design by decreasing the number of physical connections needed to achieve interconnectivity among network operators, further reducing cost. Fewer connections also mean less testing to ensure that all interoperability capabilities are working properly, further reducing administrative costs.[9]

In sum, public safety can benefit from the substantial efforts undertaken in the commercial sector to develop and implement IPX. Again the decision on whether to use a single or multiple IPX providers is within the Commission's discretion. IPX is available from multiple operators, like Syniverse. Of course, if multiple providers are used, the design of the network will inherently become more complex and costly to deploy and maintain.

IV. CONCLUSION

Syniverse commends the Commission for moving forward on the creation of an interoperable public safety broadband network and appreciates the opportunity to share its views. Based on Syniverse's experience, the roaming clearing house model and IPX solution have successfully worked in the commercial sector to facilitate roaming and interconnectivity among disparate network operators and can be utilized by public safety networks to promote efficiencies and interoperability. There is simply no need to create new standards and procedures when a secure and reliable commercial solution is available.

[9] *See, e.g.*, *Notice*, 26 FCC Rcd at 763-65 ¶¶ 109-115 (discussing the need for interoperability testing).

Respectfully submitted,

By: /s/ Jerry Easom

Jerry Easom
Vice President, Industry Relations

SYNIVERSE TECHNOLOGIES
8125 Highwoods Palm Way
Tampa, Florida 33647
(813) 637-5000

April 11, 2011